October 2016

Citizens **Information** Board
information · advice · advocacy

Volume 43: Issue 10
ISSN 0790-4290

Relate

The journal of developments in social services, policy and legislation in Ireland

Contents

Page No.

Data protection

The regulation of data in Ireland is known as *data protection*. The primary legislation in this area are the Data Protection Acts 1988 and 2003. The regulation of data is necessary in order to balance the protection of an individual's privacy rights with the rights of organisations to collect and use data for business. The Data Protection Commissioner is responsible for overseeing data protection in Ireland.

Data refers to any material, either in hard copy or digital form, which can be collected and processed. Not all data is treated the same under Irish law, and some categories of data require particularly strict regulation, for example, data about individuals.

Types of data

Personal data

Personal data is data which relates to or can identify a living person either by itself or together with other available information. Examples of personal data include a person's name, phone number, bank details and medical history. A *data subject* is the person the personal data relates to. Organisations that collect or use personal data are known as data controllers and data processors (see page 2).

Sensitive personal data

Sensitive personal data means personal data relating to any of the following:

- The data subject's racial or ethnic origin, their political opinions or their religious or philosophical beliefs
- Whether the data subject is a member of a trade union
- The data subject's physical or mental health or condition or sexual life

- Whether the data subject has committed or allegedly committed any offence
- Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings

Sensitive data should only be processed by a data controller or a data processor once certain criteria has been met.

Open data

Open data describes data held by public bodies which is made available and easily accessible online for public re-use and redistribution. The disclosure of this data can help to deliver economic, social and democratic benefits. The Irish government currently maintains a central open data portal available online at **data.gov.ie/data.**

In order to publish open data, public bodies should carry out a data audit to assess what data could potentially be released without any breach of data protection. Open data should not contain personal or sensitive data relating to individuals. Statistical data which has been compiled from personal or sensitive personal data, such as crime rates, or household deprivation statistics, may be published as open data. However, this data must be anonymised and aggregated using recognised statistical methods before being published.

Data controllers and data processors

Data controllers are defined in the Acts as persons or organisations who control the content and use of data. Examples of data controllers include medical professionals, solicitors, banks, government departments, and voluntary organisations. A local hairdresser or coffee shop may be a data controller if that business keeps customer details on file, for example, to make appointments or to operate a promotional points system.

Data processors are persons or organisations who process data on behalf of data controllers. Data processors are separate from data controllers and are not employees of the data controllers. Examples of data processors include payroll companies, market research companies and cloud computing providers, all of which may hold or process personal information on behalf of a data controller. Many data processors may also be data controllers for other information they keep such as their own employee records and marketing materials.

The Data Protection Acts apply to data controllers and data processors established in Ireland, and to data controllers and data processors established outside the European Economic Area (EEA) who make use of equipment in Ireland for processing personal data, for example, shops located outside the EEA but selling online through an Irish website.

Data protection guidelines

All data controllers must comply with the following eight data protection guidelines which have been prescribed by the Data Protection Commissioner based on the Acts. They must:

- Obtain and process the information fairly
- Keep the information only for one or more specified, explicit and lawful purposes
- Use and disclose the information only in ways compatible with these purposes
- Keep the information accurate, complete and up-to-date
- Ensure that the information is adequate, relevant and not excessive
- Retain the information for no longer than is necessary for the purpose or purposes for which it was collected
- Give the individual (data subject) a copy of their personal data, if requested
- Keep the information safe and secure

A data processor must ensure data held by them on behalf of a data controller is kept securely and no unauthorised access, use, disclosure or destruction of the data occurs.

The Acts do not set out specifically how data should be secured by specific data controllers and data processors. When determining measures that provide an "appropriate" level of security for the data, the following factors should be taken into account:

- The state of technological development
- The cost of implementing the measures
- The harm that might result from an unlawful disclosure
- The nature of the data concerned

A data controller or data processor must ensure that their employees and other persons in the workplace are aware of and follow the organisation's data protection guidelines.

To lawfully process sensitive data, a data controller or data processor must comply with the eight data protection guidelines and at least one of the following additional special conditions:

a) The data subject has given explicit consent to process their data, or

b) The processing must be necessary for one of the following reasons:

- The data controller has a legal obligation to process the personal data, for example, the Gardaí
- To prevent injury or serious loss being incurred by the data subject or another person
- It is carried out by a not-for-profit organisation in respect of its members or other people in regular contact with the organisation
- The information being processed has been made public as a result of steps deliberately taken by the data subject
- In connection with legal proceedings
- For medical purposes
- It is carried out by political parties or candidates for election in the context of an election
- For the purpose of assessment for tax liability or social welfare requirements

Registration

Some data controllers and data processors must register annually with the Data Protection Commission. The main categories of organisations required to register with the Data Protection Commissioner are:

- Government bodies and public authorities
- Banks, financial and credit institutions
- Insurance undertakings (not including brokers)
- Organisations whose business consists wholly or mainly in direct marketing
- Organisations whose business consists wholly or mainly in providing credit references
- Organisations whose business consists wholly or mainly in collecting debts
- Internet access providers
- Telecommunications networks or service providers
- Health professionals processing personal data related to mental or physical health
- Organisations processing genetic data
- Organisations whose business consists of processing personal data for the supply to others, other than journalistic, literary or artistic purposes

There is an annual fee for registering with the Data Protection Commissioner. Registering organisations must inform the Data Protection Commissioner of their methods of processing personal information. These details are published online and are publicly accessible on the website of the Data Protection Commissioner, **dataprotection.ie.**

Direct marketing and data protection

Many organisations collect personal data in order to target people with advertising. This is known as direct marketing. For example, if you filled out a form or entered a competition, you may have consented to an organisation contacting you with their advertising materials. However, unaddressed mail delivered to your home is not covered by the Data Protection Acts as no personal data is used, for example, letters addressed to "the owner" or "the occupant".

If you receive marketing materials which, to your knowledge, you did not request, these materials could be *unsolicited communications*. If you receive unsolicited communications, you can send a written request to the organisation requesting them to stop processing your data for that purpose. If the data controller collected your personal data solely for the purposes of marketing, the data controller should erase your information within 40 days of your request. If you want the data controller to keep your details for another purpose but not for marketing, the data controller must comply with this request. The data controller should inform you of your right to "opt out" of all such marketing.

If you are unsure about how your personal data was obtained by a data controller or data processor, you can request an explanation from the data controller. If the data controller does not address your concerns to your satisfaction, you can make a complaint to the Data Protection Commissioner (see page 5).

You can also object to your personal details being used for direct marketing purposes if your details were taken from the electoral register or from information made public by law, such as a shareholders' register. There is no charge for objecting. Your objection should be sent in writing to the specific data controller initially, and if you are not satisfied with their response, you can make a complaint to the Data Protection Commission.

If you do not want to receive direct marketing telephone calls, you should contact your telecoms service provider. They will make a note of your request in the National Directory Database (NDD) "opt-out" register. It is an offence to make direct marketing calls to any phone number listed in the NDD.

Organisations must get your permission before they contact you by fax machine, automated dialling, email or text message for direct marketing purposes. Any form of direct marketing which uses personal data should contain a simple "opt-out" procedure you can use to stop receiving those contacts.

Rights of data subjects

Right to establish existence of personal data

If you believe a person or organisation is keeping personal data about you, you can request that they tell you if they are keeping this information. If such information is being kept, you are entitled to request a description of the information and the purpose for which it is being kept. A data controller cannot charge you a fee for responding to such a request and you should be provided with a response within 21 days from the date that you made the request.

Right of access and restriction

If a data controller is keeping personal data about you, you can request a copy of that data. You can also ask the purpose for which your data is being kept and the names of any person or organisation who may have obtained your data from the data controller. You are also entitled to know how the data was obtained by the data controller unless it is contrary to the public interest. If the information being held is processed automatically, for example, by a computer programme, and the outcome of such processing may impact you, you can ask how the processing is carried out.

You must receive a response from the data controller within 40 days from the date of your request being made. You may be asked by the data controller to pay a fee when making a request for a copy of the data. Currently this fee may not exceed €6.35.

There are certain exceptions to this right of access to your personal data. These exceptions are in order to balance the rights of the individual with the needs of wider society. For example, a suspect would not be entitled to make a data access request in relation to data obtained and processed by the Gardaí during the investigation of a crime. And you are not entitled to access information held by a data controller about another person, for example, a spouse or parent, without the express consent of that other person.

If a data controller refuses a request for access to personal data, they must state the reasons why the request is being refused. If you are not satisfied with their response to your request, you can submit a complaint to the Data Protection Commission (see page 5).

Right to correct or erase data

If you believe a data controller is keeping personal data about you which is incorrect, you can request that this data be corrected or erased. The data controller must comply with your request as soon as possible and at least within 40 days of the request being made. The data controller must notify you that the corrections have been made to your data and they also must notify any third party to whom your data was disclosed within the last 12 months. These notifications are only required where it would not be too onerous on the data controller to do so.

If you believe that a data controller or data processor does not have a legitimate reason for processing your personal data, you can request that they stop processing that data where it could cause you damage or distress. The data controller must reply within 20 days of your request stating that they will carry out your request or that they believe your request is unwarranted.

This right does not apply if any of the following occurred:

- You already agreed that the data controller can use your details
- A data controller needs your details under the terms of a contract to which you have agreed, for example, a phone or utility services agreement
- Election candidates or political parties need your details for electoral purposes
- A data controller needs your details for legal reasons, for example, for the purposes of legal proceedings

Rights relating to automated decision making

If an organisation is making certain important decisions about you based on your personal details, this information should not be processed only by automated means, such as using a computer programme, for example, where you are being evaluated for a loan or a work promotion. The processing of your details in these situations should involve some human input and must not be automatically generated by a computer only, unless you agree to this.

Exceptions to the rights of the individual

Your personal data may be processed without your consent where it is in the interests of the security of the State or where it is required for the detection, prevention or investigation of a criminal offence. Equally, your consent is not required if the data is being processed in order to prevent injury or other damage to the health of any person or property, or is required during the course of legal proceedings.

Data Protection Commissioner

The Data Protection Commissioner is responsible for monitoring the lawfulness of data handling in Ireland. The Commissioner hears complaints from individuals about how personal data is being processed by data controllers and data processors. The Commissioner also monitors European legislation and case law in order to inform the public about changes in data protection law. The Commissioner also promotes data regulation and publishes relevant material to inform the public, data controllers and data processors about data protection laws and best practice.

Making a complaint

If you wish to make a complaint you can write to or email the Data Protection Commissioner explaining your case. Your complaint should include the following details:

- The name of the organisation or person you are complaining about
- A description of the steps you have already taken to have your concerns dealt with
- Details of any response you have received from the organisation
- Copies of any letters or emails exchanged between you and the organisation or person

The Commissioner's office will investigate your complaint and try to resolve the matter. If a resolution is not possible or forthcoming, you may ask the Commissioner to make a formal decision on whether the data controller has violated your rights. The Commissioner cannot award you compensation. If you suffer damage through the mishandling of your personal details, you may be able to claim compensation through the courts but the Commissioner has no function in these actions and cannot give you legal advice. If the Commissioner agrees with your complaint, they will take steps to make sure that the data controller or data processor obeys the law and addresses your concerns. If the Commissioner rejects your complaint, they will let you know in writing. If you are not satisfied with the Commissioner's decision, you can appeal the decision in the Circuit Court.

Enforcement

If the Commissioner thinks that an organisation is in breach of the Acts, they may give notice in writing to the organisation. This notice may request that the organisation take the necessary steps to bring the organisation into compliance with the Acts. Such a request can include asking the organisation to erase, destroy or correct data held, or that data is supplemented with a statement as directed by the Commissioner. The Commissioner's written notice will specify the time within which these steps must be taken, that is, whether it is an urgent matter or not.

Once an organisation has complied with the requirements of an enforcement notice it will notify the data subject within 40 days of becoming compliant. If the organisation does not agree with the requirements of the enforcement notice, it can appeal the notice to the Circuit Court. Failure to carry out the requirements of an enforcement notice without a reasonable excuse is a criminal offence.

Specific data controllers

Some organisations handle particular types of data which can often become the subject of complaints to the Data Protection Commissioner. Other organisations are unique, such as the Government or utility providers and they must obey specific data protection rules which only apply to them.

Medical data

Healthcare providers must strictly adhere to data protection laws. Your medical data can only be viewed by those working in the medical profession on a "need to know" basis. This applies in particular to administrative staff in hospitals and GP clinics. Your medical details can also be disclosed where there is a danger of injury to you or another person. Your medical data may be used for the purposes of research and statistical analysis but only once the data has been anonymised and aggregated. You should be consulted about this before your data is processed in this way. If a healthcare provider is keeping patient records on a computer system, then that provider should register with the Data Protection Commissioner. All patients have a right of access to their medical records except where it may cause damage to that patient's well being, for example, psychiatric notes.

Workplace data

Every employer retains some personal data about their employees, such as their name, address, wages, PPS number, performance records, and contract of employment. This means that every employer is also a data controller and must obey the Data Protection Acts.

An employer cannot request a full background check or a Garda data access request about a potential employee at interview stage. Garda vetting can take place before someone is appointed and organisations entitled to obtain Garda vetting will be registered with the Garda Síochána National

Vetting Bureau for this purpose. An employer should only request a PPS number once you have become an employee. An employer may ask to see your passport at recruitment stage but only to ensure that you are entitled to work in Ireland. Any monitoring devices in the workplace such as CCTV, computer usage logs and location tracking devices such as those used on trucks, should be disclosed to the employee and the purpose for such monitoring explained.

The Government and data sharing

Data sharing among public sector departments refers to one department, for example, the Department of Social Protection, transferring personal data to another government department or body, for example, Revenue. This practice was prohibited for a long time but in recent years it has become standard practice. The sharing of this data remains unregulated. However, the Data Protection Commissioner has made the following recommendations:

- It must have a basis in primary legislation
- It should be made clear to individuals that their data will be shared and for what purpose
- There must be a clear justification for such sharing
- Only the minimum amount of data necessary to fulfill the purpose should be shared
- Access to and disposal of shared data should have the appropriate security controls

The Government has approved the drafting of a Data-Sharing and Governance Bill which will regulate public sector sharing of data. The Bill is expected to be drafted during autumn 2016.

Telecoms and internet service providers

Telecoms and internet service providers hold vast amounts of personal data including customers' names, phone numbers, IP addresses, location data and usage data. These service providers are specifically regulated in the context of direct marketing (see page 3).

The Data Protection Commissioner can audit these service providers to assess their data management practices. If there is any breach of the security of this data, the service providers have an obligation to notify the Data Protection Commissioner within 24 hours. They must also notify the individual data subjects affected by the breach if there is likely to be any adverse consequences to them. A service provider that fails to implement reasonable security measures will be guilty of a criminal offence.

Location and traffic data refers to individuals' phone and internet usage. This data should only be processed as necessary, such as for billing, and only accessed by those authorised to do so. If you believe your data has been used or disclosed unfairly by a telecoms or internet service provider you may complain directly to that provider who should take steps to remedy the issue. If you are dissatisfied with that providers response, you can make a complaint to the Data Protection Commissioner.

Website cookies

Cookies are small files that a website asks your internet browser to store on your computer. They are put there by most websites that you visit. Websites use the information in these stored files to tailor the content of their webpage to your interests. The manner in which websites can use cookies is regulated by the European E-Privacy Directive as implemented under Irish law. The minimum requirement is that you understand clearly what you are being asked to consent to in terms of a website's use of cookies and that you have a means of giving or refusing consent to their use.

Usually when you land on a website for the first time a dialogue box will open stating that the website uses cookies and telling you their general purpose. You will then be asked to consent to the use of these cookies. All Irish-operated websites should have a *cookie policy* containing information which will allow you to make an informed choice about their usage and tell you how to manage and disable the cookies.

Right to be forgotten

The *right to be forgotten* is a right to have search engine results which relate to you or to a certain incident concerning you, removed from the search listing once that information is no longer relevant. For example, if an online search for your name turned up a link to a photograph of you which you believe is no longer relevant for the purpose for which it was collected, you can request that the search engine remove that link from their search results.

The right to be forgotten first arose in a European Court of Justice decision in May 2014. A Spanish national made a complaint through the Spanish data protection authority to have Google search results removed from search listings which referred to a previous legal case involving the plaintiff. In its ruling, the court found that Google was a data controller, processing personal information, with a corporate presence in Europe. As such, it was subject to EU data protection laws. The court found that such processing affected the plaintiff's fundamental rights to privacy and protection of his personal data. The court further concluded

that information which may have been lawfully processed initially may become unlawful when it is incompatible with the law. This may arise where the data in question is inadequate, irrelevant, excessive in relation to the purpose of the data processing, out-of-date or kept longer than necessary.

Exceptions to the rule

The right to be forgotten is not an absolute right and the following criteria will be applied by the data controller when considering requests:

- The search results must relate to an individual and must be results which are listed from a search of that person's name
- If the person is a public figure or has a role in public life the request may not be upheld
- Is the data relevant? Is there is a public interest in having the information available? If so, the request may not be upheld.
- If the data subject is a minor, the request is more likely to be upheld
- If the information is inaccurate, the request is more likely to be upheld
- If the accuracy of the information is in dispute, for example, court proceedings are ongoing, the request is less likely to be upheld
- If the data is sensitive personal data, the request is more likely to be upheld
- If the data was originally published for journalistic purposes, the request is less likely to succeed
- If the data may put the data subject in danger or at risk, it is more likely to be removed

Requests under the right to be forgotten procedure are assessed on a case by case basis by the search engine or website administrators.

The ruling applies to searches against a person's name only, not words or terms. Where a search engine operator refuses to remove a disputed link, the requester may complain to their national data protection authority. A successful request will only serve to have the website address (known as a *URL*) removed from the search results for that person's name. The content will remain on the website but the address of the page will not be searchable via the particular search engine. The right to be forgotten will only affect searches from the European version of the search site such as google.co.uk or google.ie. For example, the removed URL will not be returned when you search on google.ie but it will be available in search results carried out outside of Europe using google.com.

How to exercise your right to be forgotten

Google have produced an online request form which you can complete and submit a right to be forgotten request directly to their offices, see **support.google.com/legal**. The completed form must be accompanied by a photo ID and a signed permission from you if someone else is making the submission on your behalf. As the right to be forgotten is not absolute, Google assess every request on a case-by-case basis to decide if it meets with the requirements of the court decision. In your submission, you must give the search term, that is, your name, and state what links you want removed from future search listings and why.

You should also make similar requests to the other European-based search engines, for example, Yahoo and Bing, as these organisations must also obey the court decision. You may also make similar requests of the individual websites if they are based in Europe. If you are not satisfied with the decision of the search engine provider or website, you can make a complaint to the Data Protection Commissioner.

European data protection

Irish data protection laws are based on European legislation. As such, data protection laws across European countries are quite similar.

Safe Harbour

One European law states that personal data collected in Europe should not be transferred out of Europe, where it may go to a country which does not have the same level of data protection as Europe. The EU-US Safe Harbour framework was an agreement between the United States and Europe which allowed personal data to be transferred from Europe to the United States. Over 4,000 data controllers and data processors in Europe such as Google and Facebook all signed up to the Safe Harbour agreement.

In 2015, the case of Schrems v Facebook was heard by the European Court of Justice. The plaintiff alleged that Facebook was in breach of the Safe Harbour agreement because it was supplying personal data collected in Europe to the United States intelligence services, who in turn were using the information as part of mass surveillance programmes. Using the information in this way was beyond the purpose for which the data was obtained and was in breach of European citizens' fundamental rights. It was decided that the Safe Harbour agreement was invalid as the protection of data in the United States could not be guaranteed.

The Citizens Information Board provides independent information, advice and advocacy on public and social services through citizensinformation.ie, the Citizens Information Phone Service and the network of Citizens Information Services. It is responsible for the Money Advice and Budgeting Service and provides advocacy services for people with disabilities.

Head office
Ground Floor
George's Quay House
43 Townsend Street
Dublin 2
D02 VK65

t 0761 07 9000
f 01 605 9099
e info@ciboard.ie
w citizensinformationboard.ie

However, data may still be transferred outside of Europe regardless of the Safe Harbour agreement being declared invalid if one of the following reasons applies:

- The transfer is required or authorised by law
- The data subject consents to the transfer
- The transfer is necessary to perform a contract which is in the interests of the data subject or which the data subject wants to enter themselves
- The transfer is necessary for reasons of public interest
- The transfer is necessary for obtaining legal advice or for legal proceedings
- The transfer is necessary to prevent injury or damage to the data subject or their vital interests
- The transfer is from a publicly-available source of information, for example, a public register
- The Data Protection Commissioner has approved the transfer where the data controller can show there are adequate data protection safeguards in place

Privacy Shield

The EU-US Privacy Shield framework was finalised on 1 August 2016 and now replaces the Safe Harbour agreement. This new framework has four pillars:

- It increases the obligations on companies to publish privacy statements particularly around the onward transfer of data
- US authorities have placed explicit limitations and oversight mechanisms on the data access permissions of its public authorities and has confirmed the absence of indiscriminate mass surveillance
- The framework includes multiple redress mechanisms for data subjects including an arbitration procedure and an US-based independent ombudsman
- An annual joint review mechanism will monitor the implementation of the Privacy Shield

In order for companies to avail of the EU-US Privacy Shield they have to self-certify their compliance with the framework. Organisations can do this by completing an online application. Once approved by the EU and US authorities, organisations are registered on a publicly-accessible database. European organisations should ensure their US counterparts are registered under the Privacy Shield before transferring data to them.

General Data Protection Regulation 2016

The EU Regulation 2016/679 (General Data Protection Regulation) came into force 24 May 2016 replacing the 1995 European Data Protection Directive. The regulation allows for a two-year transition period so organisations can update their data handling policies in compliance with the Regulation which will apply from 25 May 2018.

Planned changes to current legislation

The Regulation aims to put in place a single, uniform set of data protection rules across the EU. Although the majority of its provisions are similar to current data protection laws there are some significant differences including:

- Data breaches which may result in risk to the data subject must be notified to the Data Protection Commissioner within 72 hours of the breach.
- The obligation on some organisations to register with the Data Protection Commissioner will no longer apply. Instead organisations must adopt internal policies which demonstrate compliance with data protection laws. Impact assessments will also need to be carried out before organisations begin certain processing activities.
- Various organisations, including all public authorities, must appoint a specific data protection officer to oversee compliance with the Regulation

The information in *Relate* is intended as a general guide only and is not a legal interpretation

Citizens Information

LOG ON
citizensinformation.ie

CALL
0761 07 4000 Mon to Fri, 9am to 8pm

DROP IN
260 locations nationwide